PATENT ABSTRACTS OF JAPAN

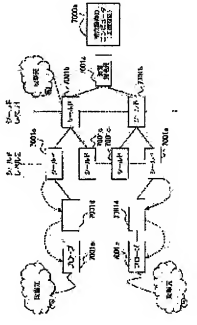
(11)Publication number : 2003-283571
(43)Date of publication of application : 03.10.2003

(51)Int.Cl. H04L 12/66
G06F 13/00
H04L 12/46

(21)Application number : 2002-079728 (71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(22)Date of filing : 20.03.2002 (72)Inventor : ERIC CHEN

(54) DEFENSIVE METHOD AND APPARATUS AGAINST DISABILITY-OF- SERVICE ATTACK, AND COMPUTER PROGRAM THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a defensive method with which defense is made possible by detecting more kinds of attacks and the communication band of a network is prevented from being wasted by traffic caused by the attack.
SOLUTION: In order to defense a computer 7000a of a person to be attacked, shields 7001b and 7001c distributed with a variable level number are located. Each of the shields analyzes a packet associated with the computer 7000a of the person to be attacked, narrows down the band of suspicious traffic by an examination and detects the attack. When the attack is detected, each shield transfers the program of a probe toward the upstream of the attack. When the packet of the attack is found out, a probe 7001e discards the packet and transfers the program of the probe toward the further upstream side.



[0044] A third specific example is to examine utilizing a distribution of source addresses of communication packets. If observing in a normal state for a certain prolonged time, the distribution of source addresses of communication packets should be almost constant. However, in case of DDoS attacking, a source address is spoofed using an address that has been randomly selected. Thus, when the variance level of source addresses is abnormally high, in other words, if randomness is high, an attack can be detected. FIG. 5(a) and (b) are graphs illustrating distribution states of source IP addresses, respectively. FIG. 5(a) illustrates a distribution example in a normal state and FIG. 5(b) illustrates a distribution example when receiving DDoS attacking. Each horizontal axis denotes IP address and each vertical axis denotes the number of appearances (or appearance frequency is also acceptable) of communication packets. As illustrated in FIG. 5(a), there is a concentrating tendency on specific addresses such that only a small number of specific source addresses have a large number of appearances while the number of appearances of communication packets for other source addresses is small or zero. By contrast, as illustrated in FIG. 5(b), in case of the DDoS attacking, addresses are randomly selected for spoofing, so that all the source addresses have uniformly the large number of the appearances. Namely, the variance level of the distribution of the number of appearances in a space of the IP addresses is large.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－283571
（P2003－283571A）
(43)公開日　平成15年10月3日(2003.10.3)

(51)Int.Cl.⁷	識別記号	Ｆ１		ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ	５Ｂ０８９
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｋ０３０
Ｈ０４Ｌ　12/46		Ｈ０４Ｌ　12/46	Ｅ	５Ｋ０３３

審査請求　有　　請求項の数16　ＯＬ　（全 22 頁）

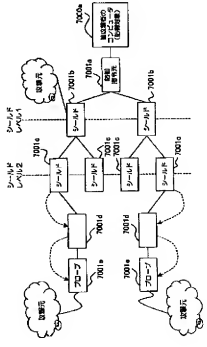
(21)出願番号　特願2002－79728(P2002－79728)
(22)出願日　平成14年３月20日(2002.3.20)
特許法第30条第１項適用申請有り

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　エリック・チェン
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100064908
弁理士　志賀　正武　（外２名）

Ｆターム(参考)　5B089 GA04 GB02 KA17 KB13 KC05 KC39 KC47 KC51 MC08 5K030 GA15 HA08 HD03 JA10 KX24 LC14 LC15 MB09 5K033 AA08 BA08 CB08 DB20 EC03

(54)【発明の名称】　サービス不能攻撃の防御方法および装置ならびにそのコンピュータプログラム

(57)【要約】
【課題】　より多くの種類の攻撃を検知して防御することのできる防御方法を提供する。また、攻撃によるトラフィックがネットワークの通信帯域を浪費しないような防御方法を提供する。
【解決手段】　被攻撃者のコンピュータ７０００ａを防御するため、可変なレベル数で分散されたシールド７００１ｂ，７００１ｃを配置する。これらシールドは、被攻撃者のコンピュータ７０００ａに関連するパケットを分析し、検査によって、疑わしいトラフィックの帯域を絞るとともに、攻撃の検出を行う。攻撃が検出されると、シールドは、プローブのプログラムを攻撃の上流に向かって転送する。プローブ７００１ｅは、攻撃のパケットを見つけるとそのパケットを破棄するとともに、さらに上流に向かってプローブのプログラムを転送する。



1

【特許請求の範囲】

【請求項１】　複数の通信装置によって構成されるネットワークに接続された防御対象コンピュータをサービス不能攻撃から防御するための防御方法であって、

前記防御対象コンピュータに最も近い通信装置であるところの境界通信装置からの指令情報に基づいて、当該境界通信装置から所定の段数分の範囲内に接続されているシールド通信装置が、当該シールド通信装置に到着する通信パケットを分析する分析処理を行い、この分析処理の結果に応じて当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである可能性に応じて当該通信パケットの優先度を決定してこの優先度に応じて当該通信パケットを転送先に転送するとともに、前記分析処理の結果当該通信パケットが確実に前記防御対象コンピュータに対する攻撃の通信パケットであることが判明した場合には当該通信パケットを破棄するシールド過程を有することを特徴とするサービス不能攻撃の防御方法。

【請求項２】　請求項１に記載のサービス不能攻撃の防御方法であって、

前記境界通信装置から最も遠い位置にある前記シールド通信装置との間の接続の段数として２以上を許容するとともに、当該段数を動的に変更できるようにしたことを特徴とするサービス不能攻撃の防御方法。

【請求項３】　請求項１に記載のサービス不能攻撃の防御方法であって、

前記シールド過程において前記通信パケットが確実に前記防御対象コンピュータに対する攻撃の通信パケットであることが判明した場合に、前記シールド通信装置がより攻撃元に近い側の隣接する通信装置に対してプローブプログラムコードを送信するプローブプログラムコード送信過程と、

前記プローブプログラムコードを受信したプローブ通信装置が、当該プローブプログラムコードを実行することによって、当該プローブ通信装置に到着する通信パケットを分析し、その結果当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである場合には当該通信パケットを破棄するとともにさらに攻撃元に近い側の隣接する通信装置に対して前記プローブプログラムコードを送信し、分析の結果一定時間攻撃のパケットが検知されない場合には前記プローブプログラムコードの処理を終了させるプローブ過程とをさらに有することを特徴とするサービス不能攻撃の防御方法。

【請求項４】　請求項３に記載のサービス不能攻撃の防御方法であって、

前記プローブ過程においては、宛先アドレスが前記防御対象コンピュータのアドレスである通信パケットを捕捉し、当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合には当該通信パケットが攻撃のパケットであると判定し、その他の場合には当該通信パケットは攻撃のパケットではないと判定することを特徴とするサービス不能攻撃の防御方法。

2

【請求項５】　請求項３に記載のサービス不能攻撃の防御方法であって、

前記プローブ過程においては、宛先アドレスあるいは送信元アドレスの少なくともいずれか一方が前記防御対象コンピュータのアドレスである通信パケットを捕捉し、

ａ）当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合、又は、

ｂ）当該通信パケットの送信元アドレスが前記防御対象コンピュータのアドレスであって且つ当該通信パケットの宛先アドレスが前記攻撃元アドレスのブロードキャストアドレスである場合、

には、当該通信パケットが攻撃のパケットであると判定し、

上記ａ）あるいは上記ｂ）のいずれにも該当しない場合には当該通信パケットは攻撃のパケットではないと判定することを特徴とするサービス不能攻撃の防御方法。

【請求項６】　請求項１に記載のサービス不能攻撃の防御方法であって、

前記シールド過程内の前記分析処理においては、予め正常時に得ておいたパラメータの値を含んだログ情報を用いて、検査時のパラメータの値と前記ログ情報とを比較することによる動的検査の処理を行うことを特徴とするサービス不能攻撃の防止方法。

【請求項７】　防御対象コンピュータをサービス不能攻撃から防御するための防御方法の処理を実行するシールド通信装置であって、

前記防御対象コンピュータに最も近い通信装置であるところの境界通信装置からの指令情報に基づいて、当該シールド通信装置に到着する通信パケットを分析する分析処理を行い、この分析処理の結果に応じて当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである可能性に応じて当該通信パケットの優先度を決定してこの優先度に応じて当該通信パケットを転送先に転送するとともに、前記分析処理の結果当該通信パケットが確実に前記防御対象コンピュータに対する攻撃の通信パケットであることが判明した場合には当該通信パケットを破棄する処理を実行することを特徴とするシールド通信装置。

【請求項８】　請求項７に記載のシールド通信装置であって、

前記分析処理においては、予め正常時に得ておいたパラメータの値を含んだログ情報を用いて、検査時のパラメータの値と前記ログ情報とを比較することによる動的検査の処理を実行することを特徴とするシールド通信装置。

【請求項９】　防御対象コンピュータをサービス不能攻撃から防御するための防御方法の処理を実行するプローブ通信装置であって、

シールド通信装置によって防御対象コンピュータに対する攻撃の通信パケットが検出されたとき、当該シールド通信装置からプローブプログラムコードを受信し、当該プローブプログラムコードを実行することによって、
当該プローブ通信装置に到着する通信パケットを分析し、その結果当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである場合には当該通信パケットを破棄するとともにさらに攻撃元に近い側の隣接する通信装置に対して前記プローブプログラムコードを送信し、分析の結果一定時間攻撃のパケットが検知されない場合には前記プローブプログラムコードの処理を終了させるプローブ過程の処理を実行することを特徴とするプローブ通信装置。

【請求項１０】　請求項９に記載のプローブ通信装置であって、
前記プローブ過程の処理においては、宛先アドレスが前記防御対象コンピュータのアドレスである通信パケットを捕捉し、当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合には当該通信パケットが攻撃のパケットであると判定し、その他の場合には当該通信パケットは攻撃のパケットではないと判定することを特徴とするプローブ通信装置。

【請求項１１】　請求項９に記載のプローブ通信装置であって、
前記プローブ過程の処理においては、宛先アドレスあるいは送信元アドレスの少なくともいずれか一方が前記防御対象コンピュータのアドレスである通信パケットを捕捉し、
ａ）当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合、又は、
ｂ）当該通信パケットの送信元アドレスが前記防御対象コンピュータのアドレスであって且つ当該通信パケットの宛先アドレスが前記攻撃元アドレスのブロードキャストアドレスである場合、
には、当該通信パケットが攻撃のパケットであると判定し、
上記ａ）あるいは上記ｂ）のいずれにも該当しない場合には当該通信パケットは攻撃のパケットではないと判定することを特徴とするプローブ通信装置。

【請求項１２】　防御対象コンピュータをサービス不能攻撃から防御するための防御方法の処理を実行する通信装置であって、
ネットワーク側から到着する通信パケットを捕捉する到着パケット捕捉部と、
前記通信パケットに対して作用を及ぼすコンピュータプログラムの処理を行うアクティブネットワーク実行環境部と、
複数のクラスにそれぞれ対応した待ち行列を備えるとともに、前記アクティブネットワーク実行環境部における前記コンピュータプログラムの処理の結果として決定されるクラスに応じて、前記通信パケットをそのクラスに対応する前記待ち行列に入れる処理を行うクラスベースの待ち行列処理部と、
前記クラスベースの待ち行列処理部が備える各々の待ち行列から順次通信パケットを取り出してネットワーク側に送出するパケット送出部と、
前記アクティブネットワーク実行環境部で実行するためのコンピュータプログラムを他の通信装置との間で転送する処理を行うプログラム転送処理部とを備えており、
前記アクティブネットワーク実行環境部は、コンピュータプログラムを記憶するコード記憶部と、このコード記憶部に記憶されたコンピュータプログラムを読み出して実行するコード実行部とを備えており、
前記コード記憶部には、
到着する通信パケットの分析を行い、この分析の結果、前記通信パケットが攻撃の通信パケットである可能性に応じて前記通信パケットのクラスを決定するとともに、当該通信パケットが確実に攻撃の通信パケットである場合には当該通信パケットを破棄する処理をコンピュータに実行させるシールドモジュールと、
到着する通信パケットを分析し、その結果当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである場合には当該通信パケットを破棄する処理をコンピュータに実行させるプローブモジュールと、
前記プローブモジュールの処理をコンピュータが実行した結果、攻撃の通信パケットが見つかった場合に、自己のプログラムコードの複製をさらに攻撃元に近い側の隣接する通信装置に対して送信する処理をコンピュータに実行させる自己複製送信モジュールと、
前記プローブモジュールの処理をコンピュータが実行した結果、攻撃の通信パケットが所定時間継続して見つからなかった場合に、自己のプログラムコードを消滅させる処理をコンピュータに実行させる自己消滅モジュールとが少なくとも記憶されていることを特徴とする通信装置。

【請求項１３】　複数の通信装置によって構成されるネットワークに接続された防御対象コンピュータをサービス不能攻撃から防御するための防御方法の処理をコンピュータに実行させるコンピュータプログラムであって、
前記防御対象コンピュータに最も近い通信装置であるところの境界通信装置からの指令情報に基づいて、当該境界通信装置から所定の段数分の範囲内に接続されているシールド通信装置が、当該シールド通信装置に到着する通信パケットを分析する分析処理を行い、この分析処理の結果に応じて当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである可能性に応じて当該通信パケットの優先度を決定してこの優先度に応じて当該通信パケットを転送先に転送するとともに、前記分析処理の結果当該通信パケットが確実に前記防御対象コンピュータに対する攻撃の通信パケットであること

が判明した場合には当該通信パケットを破棄するシールド過程の処理をコンピュータに実行させるコンピュータプログラム。

【請求項１４】　複数の通信装置によって構成されるネットワークに接続された防御対象コンピュータをサービス不能攻撃から防御するための防御方法の処理をコンピュータに実行させるコンピュータプログラムであって、到着する通信パケットを分析し、その結果当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである場合には当該通信パケットを破棄するとともにさらに攻撃元に近い側の隣接する通信装置に対して当該コンピュータプログラム自身を送信し、分析の結果一定時間攻撃のパケットが検知されない場合には当該コンピュータプログラムを終了させるプローブ過程の処理をコンピュータに実行させるコンピュータプログラム。

【請求項１５】　請求項１４に記載のコンピュータプログラムであって、

前記プローブ過程においては、宛先アドレスが前記防御対象コンピュータのアドレスである通信パケットを捕捉し、当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合には当該通信パケットが攻撃のパケットであると判定し、その他の場合には当該通信パケットは攻撃のパケットではないと判定する処理をコンピュータに実行させるコンピュータプログラム。

【請求項１６】　請求項１４に記載のコンピュータプログラムであって、

前記プローブ過程においては、宛先アドレスあるいは送信元アドレスの少なくともいずれか一方が前記防御対象コンピュータのアドレスである通信パケットを捕捉し、

ａ）当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合、又は、

ｂ）当該通信パケットの送信元アドレスが前記防御対象コンピュータのアドレスであって且つ当該通信パケットの宛先アドレスが前記攻撃元アドレスのブロードキャストアドレスである場合、

には、当該通信パケットが攻撃のパケットであると判定し、

上記ａ）あるいは上記ｂ）のいずれにも該当しない場合には当該通信パケットは攻撃のパケットではないと判定する処理をコンピュータに実行させるコンピュータプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、通信ネットワークにおいて大量の通信パケット（通信トラフィック）を被攻撃者に向けて送りつけることによって機能障害を引き起こすことを狙った攻撃を防御するための防御方法、およびその防御方法を実現する通信装置ならびにコンピュータプログラムに関する。特に、通信ネットワークにおけるサービス不能（ＤｏＳ，Denial of Service）攻撃、とりわけ分散型サービス不能（ＤＤｏＳ，Distributed Denial of Service）攻撃を防御するための技術に関する。

【０００２】

【従来の技術】近年、通信ネットワーク（具体的にはインターネット）において、しばしば著名なウェブサイトに対するＤＤｏＳ攻撃が行われ、深刻な問題となっている。なお、ＤＤｏＳ攻撃とは、その名が示す通り分散型のＤｏＳ攻撃である。ＤｏＳ攻撃とは、ネットワークに接続されたコンピュータ（ウェブサーバなど）に対して大量の通信トラフィックを送りつけるものである。ＤｏＳ攻撃には様々なタイプのものがあるが、大きく次の２つのタイプに分類される。第１のタイプは攻撃対象のコンピュータの資源を浪費することによって機能障害を引き起こすことを狙うものであり、第２のタイプはより単純に大量の通信トラフィックによって攻撃対象の通信ネットワークの帯域を浪費することを狙うものである。

【０００３】第１の従来技術として、ファイアウォール装置を用いてＤＤｏＳ攻撃を防御することが考えられる。これは、何らかの手段によって悪意のある攻撃の通信パケットの送信元アドレス（具体的にはＩＰアドレスなど）を特定できたことを前提として、ファイアウォールの外側から到着する通信パケットのうち該当する送信元アドレスを有するものをファイアウォール装置において破棄し、ファイアウォールの内側のコンピュータの資源に悪影響を及ぼさないようにするという防御方法である。

【０００４】また、第２の従来技術としては、本願発明者らが既に特許出願済の防御方法も存在する。これは、ネットワーク上で通信パケットを転送するための通信装置（具体的にはルータやスイッチなど）上に、ＤＤｏＳ攻撃を検知したり検知したＤＤｏＳ攻撃を防御したりするためのコンピュータプログラムを実行することのできる環境を設け、次のような手順で被攻撃者のコンピュータを攻撃から防御するものである。その手順とは、まず、被攻撃者のコンピュータに最も近い通信装置（境界通信装置，境界ルータ）において当該通信装置を通過する通信パケットを監視し、ＤＤｏＳ攻撃を検出するプログラムモジュールを作動させる。ＤＤｏＳ攻撃が検出されると、当該ＤＤｏＳ攻撃の通信パケットを破棄するモジュールを作動させる。そして、上位の通信装置、すなわち攻撃元に近い側の通信装置を検索するモジュールを作動させる。次に、検索された上位の通信装置に対して当該検索モジュールを送信する。そして、上位の通信装置においてさらに上位の通信装置を検索する。そのようにして、順次上位の通信装置を検索し、攻撃元に最も近い通信装置を防御位置と定める。その定められた防御位置の通信装置に対して、ＤＤｏＳ攻撃の通信パケットを破棄するモジュールを送信し、当該防御位置の通信装置

においてこのモジュールを作動させることにより防御を行う。

【０００５】

【発明が解決しようとする課題】前記の第１の従来技術では、攻撃の通信パケットはファイアウォールの位置まで届いているため、たとえ防御対象のコンピュータの資源を防御することができても、ファイアウォールに至るまでの部分での攻撃による通信トラフィックを減らすことはできず、防御対象のコンピュータにとって必要な通信帯域が浪費されてしまうという問題があった。

【０００６】また、前記の第２の従来技術でも、検知できないタイプの攻撃があるという問題があった。また、攻撃のトラフィックであることが確実に判別できない状況においては、そのような疑わしいトラフィックの存在によって、使用可能な通信帯域が狭められてしまうという問題があった。

【０００７】本願発明はこのような事情を考慮してなされたものであり、より多くの種類の攻撃を検知して防御することのできる防御方法および装置ならびにそのコンピュータプログラムを提供することを目的とする。また、さらに、単に防御対象コンピュータの資源を守るだけでなく、攻撃のトラフィックあるいは攻撃であると疑われるトラフィックによってネットワークの通信帯域が浪費されないような防御方法等を提供することを目的とする。

【０００８】

【課題を解決するための手段】上記の課題を解決するために、本発明は、複数の通信装置によって構成されるネットワークに接続された防御対象コンピュータをサービス不能攻撃から防御するための防御方法であって、前記防御対象コンピュータに最も近い通信装置であるところの境界通信装置からの指令情報に基づいて、当該境界通信装置から所定の段数分の範囲内に接続されているシールド通信装置が、当該シールド通信装置に到着する通信パケットを分析する分析処理を行い、この分析処理の結果に応じて当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである可能性に応じて当該通信パケットの優先度を決定してこの優先度に応じて当該通信パケットを転送先に転送するとともに、前記分析処理の結果当該通信パケットが確実に前記防御対象コンピュータに対する攻撃の通信パケットであることが判明した場合には当該通信パケットを破棄するシールド過程を有することを特徴とするサービス不能攻撃の防御方法を要旨とする。

【０００９】また、本発明のサービス不能攻撃の防御方法は、前記境界通信装置から最も遠い位置にある前記シールド通信装置との間の接続の段数として２以上を許容するとともに、当該段数を動的に変更できるようにしたことを特徴とする。

【００１０】また、本発明のサービス不能攻撃の防御方法は、前記シールド過程において前記通信パケットが確実に前記防御対象コンピュータに対する攻撃の通信パケットであることが判明した場合に、前記シールド通信装置が最も攻撃元に近い側の隣接する通信装置に対してプローブプログラムコードを送信するプローブプログラムコード送信過程と、前記プローブプログラムコードを受信したプローブ通信装置が、当該プローブプログラムコードを実行することによって、当該プローブ通信装置に到着する通信パケットを分析し、その結果当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである場合には当該通信パケットを破棄するとともにさらに攻撃元に近い側の隣接する通信装置に対して前記プローブプログラムコードを送信し、分析の結果一定時間攻撃のパケットが検知されない場合には前記プローブプログラムコードの処理を終了させるプローブ過程とをさらに有することを特徴とする。

【００１１】また、本発明のサービス不能攻撃の防御方法は、前記プローブ過程においては、宛先アドレスが前記防御対象コンピュータのアドレスである通信パケットを捕捉し、当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合には当該通信パケットが攻撃のパケットであると判定し、その他の場合には当該通信パケットは攻撃のパケットではないと判定することを特徴とする。

【００１２】また、本発明のサービス不能攻撃の防御方法は、前記プローブ過程においては、宛先アドレスあるいは送信元アドレスの少なくともいずれか一方が前記防御対象コンピュータのアドレスである通信パケットを捕捉し、ａ）当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合、又は、ｂ）当該通信パケットの送信元アドレスが前記防御対象コンピュータのアドレスであって且つ当該通信パケットの宛先アドレスが前記攻撃元アドレスのブロードキャストアドレスである場合、には、当該通信パケットが攻撃のパケットであると判定し、上記ａ）あるいは上記ｂ）のいずれにも該当しない場合には当該通信パケットは攻撃のパケットではないと判定することを特徴とする。

【００１３】また、本発明のサービス不能攻撃の防御方法は、前記シールド過程内の前記分析処理においては、予め正常時に得ておいたパラメータの値を含んだログ情報を用いて、検査時のパラメータの値と前記ログ情報とを比較することによる動的検査の処理を行うことを特徴とする。

【００１４】また、本発明は、防御対象コンピュータをサービス不能攻撃から防御するための防御方法の処理を実行するシールド通信装置であって、前記防御対象コンピュータに最も近い通信装置であるところの境界通信装置からの指令情報に基づいて、当該シールド通信装置に到着する通信パケットを分析する分析処理を行い、この分析処理の結果に応じて当該通信パケットが前記防御対

象コンピュータに対する攻撃の通信パケットである可能性に応じて当該通信パケットの優先度を決定してこの優先度に応じて当該通信パケットを転送先に転送するとともに、前記分析処理の結果当該通信パケットが確実に前記防御対象コンピュータに対する攻撃の通信パケットであることが判明した場合には当該通信パケットを破棄する処理を実行することを特徴とするものである。

【００１５】また、本発明のシールド通信装置は、前記分析処理において、予め正常時に得ておいたパラメータの値を含んだログ情報を用いて、検査時のパラメータの値と前記ログ情報とを比較することによる動的検査の処理を実行することを特徴とする。

【００１６】また、本発明は、防御対象コンピュータをサービス不能攻撃から防御するための防御方法の処理を実行するプローブ通信装置であって、シールド通信装置によって防御対象コンピュータに対する攻撃の通信パケットが検出されたとき、当該シールド通信装置からプローププログラムコードを受信し、当該プローブプログラムコードを実行することによって、当該プローブ通信装置に到着する通信パケットを分析し、その結果当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである場合には当該通信パケットを破棄するとともにさらに攻撃元に近い側の隣接する通信装置に対して前記プローブプログラムコードを送信し、分析の結果一定時間攻撃のパケットが検知されない場合には前記プローブプログラムコードの処理を終了させるプローブ過程の処理を実行することを特徴とするものである。

【００１７】また、本発明のプローブ通信装置は、前記プローブ過程の処理においては、宛先アドレスが前記防御対象コンピュータのアドレスである通信パケットを捕捉し、当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合には当該通信パケットが攻撃のパケットであると判定し、その他の場合には当該通信パケットは攻撃のパケットではないと判定することを特徴とするものである。

【００１８】また、本発明のプローブ通信装置は、前記プローブ過程の処理においては、宛先アドレスあるいは送信元アドレスの少なくともいずれか一方が前記防御対象コンピュータのアドレスである通信パケットを捕捉し、ａ）当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合、又は、ｂ）当該通信パケットの送信元アドレスが前記防御対象コンピュータのアドレスであって且つ当該通信パケットの宛先アドレスが前記攻撃元アドレスのブロードキャストアドレスである場合、には、当該通信パケットが攻撃のパケットであると判定し、上記ａ）あるいは上記ｂ）のいずれにも該当しない場合には当該通信パケットは攻撃のパケットではないと判定することを特徴とするものである。

【００１９】また、本発明は、防御対象コンピュータをサービス不能攻撃から防御するための防御方法の処理を実行する通信装置であって、ネットワーク側から到着する通信パケットを捕捉する到着パケット捕捉部と、前記通信パケットに対して作用を及ぼすコンピュータプログラムの処理を行うアクティブネットワーク実行環境部と、複数のクラスにそれぞれ対応した待ち行列を備えるとともに、前記アクティブネットワーク実行環境部における前記コンピュータプログラムの処理の結果として決定されるクラスに応じて、前記通信パケットをそのクラスに対応する前記待ち行列に入れる処理を行うクラスベースの待ち行列処理部と、前記クラスベースの待ち行列処理部が備える各々の待ち行列から順次通信パケットを取り出してネットワーク側に送出するパケット送出部と、前記アクティブネットワーク実行環境部で実行するためのコンピュータプログラムを他の通信装置との間で転送する処理を行うプログラム転送処理部とを備えており、前記アクティブネットワーク実行環境部は、コンピュータプログラムを記憶するコード記憶部と、このコード記憶部に記憶されたコンピュータプログラムを読み出して実行するコード実行部とを備えており、前記コード記憶部には、到着する通信パケットの分析を行い、この分析の結果、前記通信パケットが攻撃の通信パケットである可能性に応じて前記通信パケットのクラスを決定するとともに、当該通信パケットが確実に攻撃の通信パケットである場合には当該通信パケットを破棄する処理をコンピュータに実行させるシールドモジュールと、到着する通信パケットを分析し、その結果当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである場合には当該通信パケットを破棄する処理をコンピュータに実行させるプローブモジュールと、前記プローブモジュールの処理をコンピュータが実行した結果、攻撃の通信パケットが見つかった場合に、自己のプログラムコードの複製をさらに攻撃元に近い側の隣接する通信装置に対して送信する処理をコンピュータに実行させる自己複製送信モジュールと、前記プローブモジュールの処理をコンピュータが実行した結果、攻撃の通信パケットが所定時間継続して見つからなかった場合に、自己のプログラムコードを消滅させる処理をコンピュータに実行させる自己消滅モジュールとが少なくとも記憶されていることを特徴とする通信装置である。

【００２０】また、本発明は、複数の通信装置によって構成されるネットワークに接続された防御対象コンピュータをサービス不能攻撃から防御するための防御方法の処理をコンピュータに実行させるコンピュータプログラムであって、前記防御対象コンピュータに最も近い通信装置であるところの境界通信装置からの指令情報に基づいて、当該境界通信装置から所定の段数分の範囲内に接続されているシールド通信装置が、当該シールド通信装置に到着する通信パケットを分析する分析処理を行い、この分析処理の結果に応じて当該通信パケットが前記防

御対象コンピュータに対する攻撃の通信パケットである可能性に応じて当該通信パケットの優先度を決定してこの優先度に応じて当該通信パケットを転送先に転送するとともに、前記分析処理の結果当該通信パケットが確実に前記防御対象コンピュータに対する攻撃の通信パケットであることが判明した場合には当該通信パケットを破棄するシールド過程の処理をコンピュータに実行させるものである。

【００２１】また、本発明は、複数の通信装置によって構成されるネットワークに接続された防御対象コンピュータをサービス不能攻撃から防御するための防御方法の処理をコンピュータに実行させるコンピュータプログラムであって、到着する通信パケットを分析し、その結果当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである場合には当該通信パケットを破棄するとともにさらに攻撃元に近い側の隣接する通信装置に対して当該コンピュータプログラム自身を送信し、分析の結果一定時間攻撃のパケットが検知されない場合には当該コンピュータプログラムを終了させるプローブ過程の処理をコンピュータに実行させるものである。

【００２２】また、本発明は、上記のコンピュータプログラムにおいて、前記プローブ過程においては、宛先アドレスが前記防御対象コンピュータのアドレスである通信パケットを捕捉し、当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合には当該通信パケットが攻撃のパケットであると判定し、その他の場合には当該通信パケットは攻撃のパケットではないと判定する処理をコンピュータに実行させるものである。

【００２３】また、本発明は、上記のコンピュータプログラムにおいて、前記プローブ過程においては、宛先アドレスあるいは送信元アドレスの少なくともいずれか一方が前記防御対象コンピュータのアドレスである通信パケットを捕捉し、ａ）当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合、又は、ｂ）当該通信パケットの送信元アドレスが前記防御対象コンピュータのアドレスであって且つ当該通信パケットの宛先アドレスが前記攻撃元アドレスのブロードキャストアドレスである場合、には、当該通信パケットが攻撃のパケットであると判定し、上記ａ）あるいは上記ｂ）のいずれにも該当しない場合には当該通信パケットは攻撃のパケットではないと判定する処理をコンピュータに実行させるものである。

【００２４】

【発明の実施の形態】以下、図面を参照しこの発明の一実施形態について説明する。図１は、本実施形態が前提とするネットワークの構成である。図１に示すように、通信ネットワークは、複数の通信装置７００１によって接続されている。そして、通信装置７００１には１台または複数台のユーザのコンピュータ７０００を接続することができるようになっている。ユーザのコンピュータ７０００相互間で通信データのやりとりを行う際には、送信元のユーザのコンピュータ７０００が送信したパケットを通信ネットワーク上の各ノードに位置する通信装置７００１が順次転送することにより、そのパケットを宛先のユーザのコンピュータ７０００に届けるようにする。

【００２５】次に、通信装置の構成について説明する。図２は、本実施形態による通信装置７００１の内部の構成を示すブロック図である。図２に示すように、通信装置７００１は、ネットワーク（通信線）を経由して他の通信装置あるいはコンピュータから到着した通信パケットを捕捉する到着パケット捕捉部７５３１と、到着パケット捕捉部７５２１によって捕捉された通信パケットを転送するための処理を行う転送処理部７５２１と、優先度の異なる複数のクラスに対応した待ち行列（キュー）を用いることによってクラス毎の通信帯域を制御するクラスベースの待ち行列処理部７５３２と、このクラスベースの待ち行列処理部７５３２から出力されたパケットを他の通信装置あるいはコンピュータに転送するためにネットワークに送出するパケット送出部７５３３とを備えている。

【００２６】さらに、通信装置７００１は、アクティブネットワーク実行環境７５１０と、プログラム転送処理部７５４０とを備えている。アクティブネットワーク実行環境７５１０は、転送対象のパケットに対して作用するプログラムコードを実行するものであり、その内部には、プログラムコードを記憶するコード記憶部７５１２とこのコード記憶部７５１２から読み出したプログラムコードを実行するコード実行部７５１１とを有している。プログラム転送処理部７５４０は、ネットワークを介して、アクティブネットワーク実行環境７５１０で実行するためのプログラムコードを他の通信装置から受信したり、逆に他の通信装置上で実行させるためのプログラムコードを他の通信装置に対して送信したりするものである。

【００２７】アクティブネットワーク実行環境７５１０内のコード記憶部７５１２には、ＤＤｏＳ攻撃を防御するためのＤＤｏＳ攻撃防御プログラムを記憶することができるようになっている。このＤＤｏＳ攻撃防御プログラムは、センサーモジュールとシールドモジュールとプローブモジュールと自己複製送信モジュールと自己消滅モジュールとを含んでいる。センサーモジュールは当該通信装置に到着する通信パケットを継続的に分析することにより、ＤＤｏＳ攻撃の通信トラフィックが起こっているかどうかを検知する機能を有する。シールドモジュールは、センサーモジュールによる分析結果に基づき、ＤＤｏＳ攻撃の通信パケットを破棄したり、通信パケットの特徴に応じて出力のクラスを決定し当該通信パケッ

トがこのクラスに対応した待ち行列に入るようにクラスベースの待ち行列処理部７５３２に渡したりする機能を有する。プローブモジュールは、ＤＤｏＳ攻撃が検知されたときに、より上位の通信装置において、つまりより攻撃元に近い側の通信装置において防御のための処理を行う機能を有する。自己複製送信モジュールは、より上流の通信装置に、プログラム転送処理部７５４０経由でＤＤｏＳ攻撃プログラムコード自身あるいはその一部分を転送する機能を有する。自己消滅モジュールは、ＤＤｏＳ攻撃のトラフィックが継続されない状態が所定時間以上継続した場合に、ＤＤｏＳ攻撃防御プログラム自身の実行を終了したり、当該通信装置のコード記憶部上から消去したりする機能を有する。なお、防御対象のコンピュータに直接に隣接する通信装置等においては、ＤＤｏＳ攻撃防御プログラムの自己消滅を行わずに、常に少なくともセンサーモジュールだけは稼動させるようにしても良い。

【００２８】次に、この通信装置７００１が通信パケットを転送する際の処理の流れを説明する。ネットワーク側から到着した通信パケットは到着パケット捕捉部７５３１によって捕捉され、転送処理部７５３１に渡される。転送処理部７５３１は、通信パケットの宛先アドレス等に応じて、当該通信パケットをそのままクラスベースの待ち行列処理部７５３２に渡すか、あるいは当該通信パケットをアクティブネットワーク実行環境７５１０上で稼動するプログラムに渡す。このプログラムは、所定の処理を行い、通常は通信パケットをクラスベースの待ち行列処理部７５３２に渡すが、前記のようにそれがＤＤｏＳ攻撃の通信パケットであると認識された場合などはその通信パケットをそのまま破棄する場合もあり得る。クラスベースの待ち行列処理部７５３２に渡された通信パケットは、指定されたクラスの待ち行列に一旦入れられ、クラス毎に待ち行列から通信パケットが順次取り出され、パケット送出部７５３３に渡される。パケット送出部７５３３は、通信パケットをネットワーク上の所定の転送先に向けて送出する。

【００２９】次に、上述した通信装置間士が協調的に動作することによりネットワーク全体を通してＤＤｏＳ攻撃を防御する方法の概略を説明する。図３は、本実施形態による防御のしくみを示す論理的概略図である。図３において、符号７０００ａは被攻撃者のコンピュータである。被攻撃者のコンピュータ７００１ａとなる可能性があるのは、例えば、著名なウェブサイトのサーバコンピュータなどであり、このコンピュータ７０００ａがＤＤｏＳ攻撃を受けたときに防御のしくみが働く。また、７００１ａ～７００１ｅは、それぞれネットワークを構成する通信装置（具体的にはルータやスイッチなど）であり、図２を用いて説明した通信装置７００１に相当するものである。

【００３０】これらの通信装置（７００１ａ～７００１ｅ）のうち、通信装置７００１ａは、被攻撃者のコンピュータ７０００ａに直接に隣接するものであり、つまり被攻撃者のコンピュータ７０００ａ側から見てネットワークへの接点となるものであり、このような位置付けの通信装置を「境界（edge）通信装置」と呼ぶことにする。そして、この境界通信装置が防御指令元としての役割、つまりこの防御のしくみ全体を制御する中心としての役割を果たす。また、通信装置７００１ｂおよび７００１ｃ（シールド通信装置）は、防御指令元からの指令に基づき通信トラフィックを検査するとともに、ＤＤｏＳ攻撃の通信パケットを破棄するなど、シールドとしての役割を果たす。また、通信装置７００１ｅ（プローブ通信装置）は、シールドからさらに上位において防御を行うためのプローブとしての役割を果たす。

【００３１】各通信装置の、防御指令元、シールド、およびプローブとしての、それぞれの具体的な処理内容を以下に記載する。防御指令元が行う処理のひとつはシールドレベルの設定である。ここで、シールドレベルとは、防御指令元から見て、ネットワークの外側への通信装置の接続の段数（深さ）である。図３に示している構成では、シールドレベルは「２」に設定されているため、防御指令元の通信装置７００１ａから見て１段目の通信装置７００１ｂおよび２段目の通信装置７００１ｃがシールドの役割を果たす。図３ではシールドレベルが「２」に設定されている例を示しているが、他のレベルに設定することも可能であり、また動的にレベルを変更することも可能である。例えば、被攻撃者のコンピュータ７０００ａへの攻撃の度合いが大きい場合にはシールドレベルが高くなるように動的に変更することができる。また、防御指令元は、防御指令元から転送され他の通信装置上で稼動する全てのシールドモジュールに対する制御を行う。また、防御指令元は、必要に応じて稼動中のシールドモジュールの動作を停止させることもできる。

【００３２】後述するように、シールドモジュールは各通信装置（７００１ｂ，７００１ｃ）上で、局所静的検査と局所動的検査の２つのタイプの検査を行うため、ある種の攻撃はシールドモジュールによって効果的に防御することができる。しかしながら、他の攻撃の中には、ネットワーク全体の状況のデータを分析することによってはじめて検出され得るものもある。そこで、防御指令元は、大域的動的検査の処理を行う。

【００３３】本実施形態による防御をネットワークに適用した場合、最初は、防御指令元は学習段階の処理を行う。この学習段階の処理では、定期的に到着パケット（通信トラフィック）のスナップショットデータを取得し、このスナップショットデータに統計的処理を施すことによって、正常状態におけるネットワークの特徴データを取得する。この特徴データは、防御対象のコンピュータの使用目的等に応じてネットワーク毎に異なる特徴

のパターンを表わすものである。この正常状態における特徴データを便宜的に「指紋データ」と呼ぶことにする。

【００３４】学習段階で指紋データが得られると、次の段階では、防御指令元は、この指紋データを使うことによって異常を検出することができる。ここで検出可能な異常とは、例えば、到着パケットのヘッダ部分に格納されている送信元アドレスの分布が異常にばらついている（ランダム性が高い）といったものであり、このような異常が検出されるということは、ランダムに選択されたアドレスによって送信元アドレスを偽装したパケットを用いた攻撃が行われていることを示唆している。一旦ある異常が検出されると、防御指令元は、新しいパケットフィルタリングのルールを全てのシールドに対して発行することができる。

【００３５】次に、シールド（図３における通信装置７００１ｂおよび７００１ｃが果たす役割）の具体的な処理内容について説明する。シールドは、ＤＤｏＳ攻撃に対処するための「第一段階」の対応の役割を果たすように設計されている。各通信装置上において、シールドモジュールは、防御対象となっているコンピュータに向けて転送されてくる通信パケットをモニタする。これは、後述するアクティブネットワークのしくみにおいて、特定の通信アドレス（ＩＰアドレス）を有するパケットをトリガーとしてアクティブネットワーク実行環境上の特定のプログラムコードを呼び出すことによって可能となる。従って、シールドモジュールの制御は、本モジュールの所有者に関するすべての通信パケットに及ぶこととなる。

【００３６】図４は、シールドモジュールによる通信パケットのクラス分けの処理の概要を示す概略図である。図示するように、シールドモジュールの処理対象となる通信パケットは、ネットワーク側から入力インタフェースを介して到着すると、一旦入力待ち行列に入れられ、順次シールドモジュールに渡される。また、クラスベースの待ち行列処理部７５３２は、出力（ネットワークへの送出）の優先度がそれぞれ「高」、「中」、「低」の３つの待ち行列を有している。そして、クラスベースの待ち行列処理部７５３２は、アクティブネットワーク実行環境７５１０上で稼動するシールドモジュールによって決定されたクラスに応じた待ち行列に通信パケットを格納し、各待ち行列から順次通信パケットを取り出して出力する。

【００３７】各通信装置上で稼動するシールドモジュールは、通信トラフィックをクラス別に分類するクラス分け機能を有しており、このクラス分け機能は、到着した通信パケットがＤＤｏＳ攻撃の泯ホトラフィックをなすものである確率を求めることができるようになっている。そして、ＤＤｏＳ攻撃である可能性が最も高い部類に属する通信パケット、つまり最も疑わしいクラスの通信パケットは、最も優先度の低い待ち行列（「低」）に入るように指定され、クラスベースの待ち行列処理部７５３２に渡される。逆に、ＤＤｏＳ攻撃である可能性が最も低い部類に属する正常な通信パケットは、最も優先度の高い待ち行列（「高」）に入るように指定される。疑わしさの度合いが中間のクラスの通信パケットは、優先度が「中」の待ち行列に入るように指定される。

【００３８】シールドモジュールが、上記のようにクラスベースの待ち行列を用いた出力の処理を行うことにより、次の２つの効果が得られる。第１の効果は、防御対象のコンピュータが攻撃を受けている途中、疑わしい通信トラフィックが防御対象のコンピュータに到達しにくくする一方で、正常である可能性の高い通信トラフィックが防御対象のコンピュータに到達する可能性を高めることができる点である。つまり、疑わしい通信トラフィックの帯域を抑え、正常な通信トラフィックの帯域を確保することができる。第２の効果は、ＤＤｏＳ攻撃を検出するためのアルゴリズムにより柔軟性と正確性を与えることができる点である。

【００３９】従来技術においてＤＤｏＳ攻撃の通信パケットであるか否かを二値的に判断して処理していたのに比べると、上記の２つの効果は防御の方法を大幅に改善するものであると言える。何故ならば、通常時の通信トラフィックよりも広い帯域を占める通信トラフィックが流れているときに、その通信トラフィックがＤＤｏＳ攻撃によって引き起こされているものであるのか、正常な通信の量がたまたまピークをむかえているものであるのかを判別するのは、単純に行える問題ではないからである。また、たとえＤＤｏＳ攻撃であることが確認された状況下であっても、ＤＤｏＳ攻撃による泯ホパケットと正当な通信パケットとを高い信頼性で分別することは困難だからである。つまり、正常な通信パケットまでもが届きにくくなるというダメージを最小化するためには、検知アルゴリズムは、二値的な真か偽かの判断を行うものであるよりも、攻撃の通信パケットである可能性（確率）算出するものであるほうが望ましいといえる。そして、攻撃の通信パケットである可能性が非常に高い通信パケットだけを破棄するようにすべきである。

【００４０】シールドモジュール内の前記クラス分け機能は、以下に述べるように、局所静的検査と局所動的検査との２つのタイプの検査を行う。局所静的検査は、状態に基づかずに行われる検査であり、それぞれの多くの静的なパラメータに基づいて各々の到着パケットに対して行われる検査である。ここで、静的なパラメータとは、通信パケットの送信元アドレスや宛先アドレス、ヘッダ（具体的にはＩＰヘッダなど）に含まれる通信プロトコル上のパラメータ、通信パケット長、宛先ポート番号、ＩＣＭＰ（インターネット・コントロール・メッセージ・プロトコル）タイプなどである。

【００４１】例えば、防御対象のコンピュータがウェブ

サイトのサーバである場合には、その防御対象のコンピュータが他のコンピュータに対して「ｐｉｎｇ」要求を送信することはないため、シールドは、その防御対象のコンピュータに向けたタイプ０のＩＣＭＰパケット（エコー応答）や送信元のポート番号が７であるＵＤＰ（ユーザ・データグラム・プロトコル）を、検出次第すぐに破棄することができる。また、静的検査によって検出可能な他の異常の例としては、送信元アドレスと宛先アドレスが同一である通信パケットである。このような通信パケットは、そのアドレスを有するコンピュータが通信パケットの送受信のループに陥ることを狙った攻撃であるので、シールドはこのような通信パケットを全て破棄すべきである。

【００４２】局所動的検査は、状態に基づいて行われる検査であり、シールドによって記録されたログファイル（ログ情報）を用いて行われる検査である。このログファイルは、異常を検出するために用いられるデータとして、ある種のパラメータの値を所定期間にわたって記録し保持するものである。

【００４３】ここで、動的検査の具体例について説明する。第１の具体例は、異常なパケットあるいは疑わしいパケットが継続的に流入してくるときに、その継続時間を検査するものである。例えば、突然、同じ送信元から規定の最大サイズの通信パケットが５分間に渡って継続的に流入してきた場合になどには、シールドはその送信元アドレスからの通信パケットの疑わしさの度合いを上げ、その送信元アドレスからの通信パケットを「低」優先度の出力待ち行列に入れるようにする。第２の具体例は、特定のコンピュータへの到着パケットとそのコンピュータからの送出パケットの間の量（パケット数、データ量など）の比率を用いて検査を行うものである。一般にこの到着・送出間の比率は、コンピュータ（システム、例えばウェブサイトのシステム）毎に異なるが、あるコンピュータについて見た場合、その比率はほぼ一定している。そこで、予め通常時に長期的な到着・送出間の平均比率を算出しておく。そして、その平均比率に基づいて、異常を検知するための到着・送出間の比率の閾値を決定しておく。そして、検査中に到着・送出間の比率がこの閾値をこえた場合に異常とみなすことができる。なお、上限値と下限値を予め決定しておき、到着・送出間の比率が上限値を上回った場合あるいは下限値を下回った場合に異常とみなすようにしても良い。

【００４４】第３の具体例は、通信パケットの送信元アドレスの分布を利用して検査を行うものである。正常な状況においてある程度の長い期間にわたって見た場合、通信パケットの送信元アドレスの分布はほぼ一定しているはずである。ところがＤＤｏＳ攻撃が行われる際には、ランダムに選ばれたアドレスを用いて送信元アドレスの偽装が行われるため、送信元アドレスのばらつき度合いが異常に高い場合、言い換えればランダム性が高い場合に、攻撃を検出することができる。図５（ａ）および（ｂ）は、それぞれ送信元ＩＰアドレスの分布状況を示すグラフである。図５（ａ）は正常時の分布例を示しており、同（ｂ）はＤＤｏＳ攻撃を受けているときの分布例を示しており、それぞれ横軸はＩＰアドレス、縦軸は通信パケットの出現回数（あるいは出現頻度でも良い）を表している。図５（ａ）に示すように、正常時には、特定の少数の送信元アドレスの通信パケットのみの出現回数が多く、他の送信元アドレスの通信パケットの出現回数は少なかったりゼロであったりするなど、特定のアドレスに出現回数が集中する傾向がある。それに対して図５（ｂ）に示すように、ＤＤｏＳ攻撃が行われているときには、偽装のためのアドレスがランダムに選択されるために、すべての送信元アドレスについて一様に出現回数が多い。つまり、出現回数の分布がＩＰアドレスの空間にばらついている度合いが大きい。

【００４５】このようなランダム性を数値化に扱う方法を説明する。存在するすべてのＩＰアドレスの数をｋとする。ｉ番目（１≦ｉ≦ｋ）のＩＰアドレスの出現頻度を長期間にわたって測定しておくことによって、所定期間中に期待されるｉ番目の出現回数ｅ（ｉ）を予め得ておく。そして、検査時に所定期間中に実際にｉ番目のＩＰアドレスが出現した回数ｏ（ｉ）を得ておく。そして、すべてのＩＰアドレスについて、

ｄ（ｉ）＝（（ｏ（ｉ）－ｅ（ｉ））＾２）／ｅ（ｉ）

を計算し、１≦ｉ≦ｋであるすべてのｉについてのｄ（ｉ）の総和を計算する。この総和が予め定めた閾値を上回った場合に、異常とみなすことができる。

【００４６】以上説明した３種類の具体例の他にも、通信パケット長や、ＴＴＬ（Ｔｉｍｅ-Ｔｏ-Ｌｉｖｅ）値など様々なパラメータを用いた検査が可能であり、これらのパラメータ値のランダム性が異常に高い場合や、逆に一定している度合いが異常に高い場合などを検出することによって、ＤＤｏＳ攻撃が行われているかどうかを検査することができる。

【００４７】図３に示したように、シールドを複数の通信装置に分散させることにより、次の２つの効果が得られる。第１の効果は、ＤＤｏＳ攻撃を吸収しやすくなり、異常な通信トラフィックの増加を起こりにくくすることができる点である。第２の効果は、通信トラフィックの検査を異なった複数の場所で行える点である。

【００４８】次に、プローブ（図３における通信装置７００１ｅが果たす役割）の具体的な処理内容について説明する。本実施形態の防御方法は、ＤＤｏＳ攻撃によって引き起こされるダメージを最小化することを目的として、シールドを用いた防御のほかに、さらにプローブを用いる。前述のようにシールドが「第一段階」の対応の役割を果たすように設計されていたのに対して、プローブは、トレースバックおよび「第二段階」の対応の役割を果たすように設計されている。つまり、シールド過程

において通信パケットが確実に防御対象コンピュータに対する攻撃の通信パケットであることが判明した場合に、シールド通信装置がより攻撃元に近い側の隣接する通信装置に対してプローブプログラムコードを送信するプローブプログラムコード送信過程の処理が行われる。また、前記プローブプログラムコードを受信したプローブ通信装置が、当該プローブプログラムコードを実行することによって、当該プローブ通信装置に到着する通信パケットを分析し、その結果当該通信パケットが防御対象コンピュータに対する攻撃の通信パケットである場合には当該通信パケットを破棄するとともにさらに攻撃元に近い側の隣接する通信装置に対して前記プローブプログラムコードを送信し、分析の結果一定時間攻撃のパケットが検知されない場合には前記プローブプログラムコードの処理を終了させるプローブ過程の処理が行われる。

【００４９】本実施形態の防御のしくみがＤＤｏＳ攻撃を確認して、攻撃による洪水トラフィックを完璧に阻止することを決定した場合には、プローブが洪水トラフィックの元に向かって送り込まれる。その目的は次の２つである。第１の目的は、洪水トラフィックを可能な限り上流で阻止することによって、ネットワークの帯域を少しでも多く確保することである。また、第２の目的は、法的に使用する目的の攻撃の証拠を収集することである。このプローブもまた、アクティブネットワークのアクティブコードとして実現されている。つまり、プローブモジュールは、下流から上流に向かって通信装置から通信装置を段階的に移動していくエージェントのようなふるまいをする。なお、本実施形態では、次に述べるＡ型とＢ型との２つのモデルのＤＤｏＳ攻撃に対応できるように、プローブモジュールのアルゴリズムを設計している。

【００５０】まず、Ａ型のＤＤｏＳ攻撃について説明する。図６は、Ａ型のＤＤｏＳ攻撃を示す概略図である。このＡ型のモデルでは、マスター（攻撃元のコンピュータ）と、このマスターによって侵入されたスレーブ（コンピュータ）とによって攻撃が行われる。マスターコンピュータはＤＤｏＳ攻撃のプログラムをスレーブコンピュータにアップロードする。このマスターとスレーブとの間の通信をコントロールトラフィックと呼ぶ。そして、それぞれのスレーブコンピュータは、被攻撃者のコンピュータに対して膨大な量のパケットを送りつける。このとき、被攻撃者が攻撃元を特定できないようにすることを目的として、スレーブコンピュータから被攻撃者のコンピュータに対して送られる通信パケットの送信元アドレスの偽装が行われることもしばしばある。

【００５１】次に、Ｂ型のＤＤｏＳ攻撃について説明する。図７は、Ｂ型のＤＤｏＳ攻撃を示す概略図である。例えば「Ｓｍｕｒｆ」や「Ｆｒａｇｇｌｅ」を用いたＤＤｏＳ攻撃はこのＢ型に含まれる。Ｂ型の攻撃の特徴は

被攻撃者のコンピュータのダメージを大きくするために、ネットワークを用いて通信トラフィックの増幅を行う点にある。マスター（攻撃元のコンピュータ）がスレーブコンピュータに対して指令を行うことにより、スレーブコンピュータはＩＣＭＰエコー要求パケットやＵＤＰの７番ポート（エコー）のパケットをいくつかのネットワークに対してブロードキャストする。このとき各々のエコー要求のパケットの送信元アドレスは偽装されており、被攻撃者のコンピュータのアドレスが送信元アドレスとして格納されている。従って、エコー要求パケットのブロードキャスト先のネットワークに接続されたすべてのコンピュータ（正当なユーザのコンピュータ）は、被攻撃者のコンピュータに対してエコー応答のパケットを送信しようとする。このようにして、ネットワークにおいて増幅された洪水トラフィックが被攻撃者のコンピュータに向かうこととなる。

【００５２】次に、プローブによる前記Ａ型のＤＤｏＳ攻撃への対応の処理について説明する。一般に、あるひとつの通信パケットの送信元アドレスが偽装されているか偽装されていないかを見分けることはできない。そこで、初期的には、全ての通信パケットの送信元アドレスが偽装されているものという仮定を置くことにする。

【００５３】図８は、Ａ型のＤＤｏＳ攻撃に対応するためのプローブのアルゴリズムを記述した擬似プログラムコードである。以下、図８を参照しながら説明する。シールドモジュールによって検出された攻撃トラフィックの送信元アドレスが変数「ａｔｔＳｒｃ」に格納されている。本実施形態においては、アクティブネットワーク実行環境で実行される各アクティブコードは特定の所有者によって所有され、当該所有者に関するすべての通信パケットをフルに制御することができるようにオーソライズされていることを前提としている。従って、各通信装置上では、プローブモジュールは当該プローブモジュールの所有者に関するパケットをすべて捕捉し処理対象とすることができる。

【００５４】図３に示したように、シールドの通信装置からスタートして、順次自己複製送信モジュールの機能によって、攻撃元の方向に向かって隣接する通信装置に段階的にプローブモジュールの複製が転送されていく。図８に示すプローブモジュールのコードは、新たなノード（通信装置）ｕに到着して実行が開始される。

【００５５】まず図８に示す擬似コードの１行目において、変数「ｅｘｐｌｏｒｅｄ」に値「ｆａｌｓｅ（偽）」が格納される。次に同擬似コードの２行目から１１行目までのループ（ｄｏ－ｗｈｉｌｅ）が実行される。同擬似コードの３行目において、関数「ｃａｐｔｕｒｅＰａｃｋｅｔＢｙＤｅｓｔ（）」の機能によって、被攻撃者のコンピュータのアドレス（ＩＰアドレス）を宛先アドレスとする通信パケットを捕捉し、その通信パケットのデータを変数（構造体）「ｐ」に格納する。同

擬似コードの４行目において、変数「ｐ」に格納された通信パケットの送信元アドレス（ｐ．ｓｒｃ）が前記変数「ａｔｔＳｒｃ」の値に等しいならば、つまり攻撃トラフィックの送信元アドレスに等しいならば、５行目から９行目までの処理が実行される。そうでない場合には、１０行目の関数「ｒｅｌｅａｓｅＰａｃｋｅｔ（ｐ）」の機能によって当該通信パケットがリリースされる、つまり転送先の通信装置に向けて送出される。４行目の処理において攻撃トラフィックの通信パケットであると判別された場合は、同擬似コードの５行目において、関数「ｄｉｓｃａｒｄ（ｐ）」の機能により、変数「ｐ」に格納された通信パケットは破棄される。つまり、攻撃のトラフィックがここで阻止される。また、同擬似コードの７行目から９行目の処理においては、当該ノードｕに隣接するノードであって当該ノードｕに対してプローブモジュールを送信した元のノードではないもの、つまりすべての上流のノードｖ（通信装置、複数の場合もある）に対してプローブモジュール自身の自己複製を転送する。

【００５６】同擬似コードの１１行目の条件式において、攻撃のトラフィックが見つからない状態が所定時間続いた場合には、２行目から１１行目までのループを抜け出し、１２行目において自己消滅モジュールの機能によって自己を消滅させる。つまり、一旦プローブとして動作を始めたものその通信装置が攻撃の上流の位置にない場合には、プローブとしての役割を終える。

【００５７】以上説明したように、図８に示したアルゴリズムの目的は攻撃元に最も近い位置の通信装置を見つけ出し、その位置において不必要なトラフィックを阻止することである。これによって、下流に攻撃の通信パケットが流れることを防ぎ、途中の通信装置に不要な負荷がかからないようにすることができる。また、攻撃元に最も近い通信装置に到達すると、プローブはその位置情報（ＩＰアドレスなど、証拠情報）を防御指令元に報告する処理を行う。

【００５８】次に、プローブによる前記Ｂ型のＤＤｏＳ攻撃への対応の処理について説明する。前述したように、Ｂ型のＤＤｏＳ攻撃においては、攻撃元（スレーブ）から増幅のために用いられるネットワークに対して送られる通信パケットは偽装された送信元アドレスを有している。ところが、増幅のために用いられたネットワークに属しているコンピュータから被攻撃者のコンピュータに送られる洪水トラフィックの通信パケットのヘッダには、各コンピュータの正規の送信元アドレスが格納されている。シールドは、初期のには、増幅のために用いられたネットワークに属するコンピュータのアドレスを変数「ａｔｔＳｒｃ」に格納してしまうため、図８で示したアルゴリズムを使っている限りにおいては、プローブは増幅のために用いられたネットワークまでしか到達することはできず、その先、つまり真の攻撃者にさらに近い通信装置へプローブを送り込むことはできない。そこで、Ｂ型のＤＤｏＳ攻撃に対応するためのプローブとして新たなアルゴリズムを用いることにする。

【００５９】図９は、Ｂ型のＤＤｏＳ攻撃に対応するためのプローブのアルゴリズムを記述した擬似プログラムコードである。以下、図９を参照しながら説明する。図９に示す擬似プログラムコードの特徴は、その３行目と４行目の処理にある。同コードの３行目では、関数「ｃａｐｔｕｒｅＰａｃｋｅｔＡｓｓｏｃｉａｔｅｄＷｉｔｈ（）」の機能によって、被攻撃者のコンピュータのアドレスに関する通信パケットを捕捉する。つまり、例えば、送信元アドレスあるいは宛先アドレスのいずれかが被攻撃者のコンピュータのアドレスと同一である通信パケットを捕捉する。また、同コードの４行目のｉｆ文による判断のための条件式は、捕捉された通信パケットの送信元アドレスが変数「ａｔｔＳｒｃ」に等しい場合だけでなく、送信元アドレスが被攻撃者のコンピュータのアドレスであって且つ宛先アドレスが変数「ａｔｔＳｒｃ」に格納されているアドレスのブロードキャストアドレスである場合にも、その値が「真」となるように記述されている。例えば、変数「ａｔｔＳｒｃ」に格納されている攻撃元のＩＰアドレスが「１０１．１０２．１０３．１０４」であったとき、「１０１．１０２．１０３．２５５」はそのブロードキャストアドレスである。４行目のｉｆ文の条件式をこのようなものにすることにより、被攻撃者のコンピュータのアドレスが送信元アドレスであって且つ増幅に用いられているネットワークのブロードキャストアドレスが宛先アドレスであるような通信パケット、すなわち攻撃元（図７におけるスレーブ）から増幅のためのネットワークに対して送られている偽装の通信パケットを破棄できる（同コード５行目の処理）ようになるとともに、さらに攻撃元に近い通信装置にプローブモジュールを送り込むことができる（同コードの６行目～９行目の処理）ようになる。

【００６０】なお、変数「ａｔｔＳｒｃ」に格納される攻撃元のＩＰアドレスは複数のアドレスであっても良い。また、通信装置から通信装置へプローブが移動するのに伴って、この攻撃元ＩＰアドレスの情報も渡されるようにする。

【００６１】なお、上述した防御のしくみが機能するためには、必ずしもネットワークを構成するすべての通信装置がアクティブネットワーク実行環境を備えていることが要求されるわけではない。つまり、ネットワークがアクティブノードのみから構成されるのではなく、アクティブノードと非アクティブノード（アクティブネットワーク実行環境を備えず通信パケットの転送のみを行う通信装置のノード）とが混在していても良い。この場合には、ＤＤｏＳ攻撃防御プログラムコードは、アクティブノード相互間で転送され、アクティブノードにおいてのみ実行される。そして、非アクティブノードは、単に

通信パケットを転送する役割を果たす。

【００６２】次に、図１０～図１３を参照しながら、本実施形態が前提としているアクティブネットワークの実現方式の一例について説明する。

【００６３】図１０は、通信装置７００１の内部の構成を示すブロック図である。図１０に示すように、通信装置７００１には通信線７０２４ａ、７０２４ｂ、７０２４ｃ、７０２４ｄが接続されており、通信装置７００１はこれらの通信線を介して隣接する他の通信装置との間でパケットを交換することができるようになっている。また、通信装置７００１には、上記の各通信線７０２４ａ～７０２４ｄに対応したインタフェース部７０２３ａ～７０２３ｄと、パケットを転送する処理を行うための転送処理部７０２１と、パケットの転送の際の転送先の情報を記憶する転送先テーブル７０２２と、アクティブパケットに対する処理を行うためのアクティブネットワーク実行環境（Active Network Execution Environment）７０１０とが設けられている。なお、アクティブネットワーク実行環境７０１０は、内部に、アクティブコード（プログラム）を実行するためのコード実行部７０１１と、アクティブコードを記憶しておくためのコード記憶部７０１２とを備えている。なお、ここでアクティブコードとは、アクティブネットワークにおいてパケットに対する作用を行うコンピュータプログラムのコードである。

【００６４】ここで、図１０を参照しながら、この通信装置７００１の動作例の概要を説明する。隣接する他の通信装置から通信線７０２４ｄを介してパケットが到着すると、インタフェース部７０２３ｄがそのパケットを受信し転送処理部７０２１に渡す。転送処理部７０２１は、渡されたパケットのヘッダ部分に格納されている送信元（source）アドレスと宛先（destination）アドレスとを読み取り、さらにそれらのアドレスをキーとして転送先テーブル記憶部７０２２に記憶されている転送先テーブルを参照することによって、そのパケットにどう対処するかを決定する。

【００６５】パケットへの対処は大きく２通りに分けられる。そのパケットに対してアクティブコードを適用する場合と、そのパケットをそのまま他の通信装置に転送する場合とである。転送先テーブルを参照した結果、そのパケットに対してアクティブコードを適用すべきものである場合には、転送処理部７０２１は、そのパケットをアクティブネットワーク実行環境７０１０に渡す。アクティブネットワーク実行環境７０１０においては、コード実行部７０１１がそのパケットを受け取り、そのパケットに対して適用すべきアクティブコードをコード記憶部７０１２から読み出して実行する。なお、コード実行部７０１１は、アクティブコードを実行した結果、必要な場合には処理対象となったパケットを再び転送処理部７０２１に渡して他の通信装置に対して転送することもある。転送先テーブルを参照した結果、そのパケットにアクティブコードを適用せずそのまま他の転送装置に転送するべきものである場合には、転送処理部７０２１は、適切な転送先に対応したインタフェース部（７０２３ａや７０２３ｂや７０２３ｃなど）に渡し、そのインタフェース部が通信線（７０２４ａや７０２４ｂや７０２４ｃなど）を介してパケットを他の通信装置に転送する。

【００６６】なお、ここでは通信線７０２４ｄを介して他の通信装置からパケットが到着した場合を例として説明したが、他の通信線を介してパケットが到着した場合の処理も同様である。

【００６７】次に、通信装置７００１内の転送処理部７０２１がいかにしてパケットに対する処置（アクティブコードを適用するか、単純に他の通信装置に転送するか）を決定するかを具体的に説明する。

【００６８】本実施形態が基礎とするフレームワークでは、アクティブネットワーク実行環境はパケットの中において指定されているＩＰアドレスに基づいて起動される。ここで、全ての（グローバル）ＩＰアドレスの集合をＩと表わすものとする。また、送信元ＩＰアドレスがｓであり宛先ＩＰアドレスがｄであるようなパケットを（ｓ，ｄ）と表わすものとする。また、通信装置のアクティブネットワーク実行環境に格納されているすべてのアクティブコードはそれぞれ特定のユーザに属するものとし、ある特定のユーザの所有するＩＰアドレスの集合をＯと表わすものとする。

【００６９】本フレームワークでは、上記特定のユーザに属する個々のアクティブコードは、次に示す式による集合Ａで表されるパケットであって、かつ当該アクティブネットワーク実行環境を備えた通信装置（ノード）によって受信されたパケットに対してアクセスする権限を持つ。すなわち、

Ａ＝｛（ｓ，ｄ）∈［（Ｏ×Ｉ）∪（Ｉ×Ｏ）］｜ｓ≠ｄ｝

である。つまり、この式が意味するところの概略は、特定のユーザに属するアクティブコードは、当該ユーザが所有する全てのＩＰアドレスのいずれかを送信元または宛先のアドレスとするようなパケットに対してアクセス権を有するということである。

【００７０】当該ユーザに属するｎ個のアクティブコードがある通信装置（ノード）に格納されているとき、ｉ番目（１≦ｉ≦ｎ）のアクティブコードは、集合Ｃ（ｉ）（Ｃ（ｉ）⊆Ａ）に属するパケットをキャプチャーして処理することをアクティブネットワーク実行環境に対して予め要求しておく。つまり、当該ユーザに関して、アクティブネットワーク実行環境は、ｃ（１）∪ｃ（２）∪・・・・・∪ｃ（ｎ）なる和集合の要素であるパケット（ｓ，ｄ）によって起動されるものであり、このようなパケットを「アクティブパケット」と呼ぶこ

とができる。

【００７１】図１１は、図１０に示した転送先テーブル記憶部７０２２に記憶されている転送先テーブルの一例を示す概略図である。上記のフレームワークを実現するために必要な情報は、このような転送先テーブルに格納することが可能である。

【００７２】図１１に示すように、転送先テーブルは、タイプ（Type）と宛先アドレス（Destination ）と送信元アドレス（Source）と転送先（Send to ）の各項目を含んでいる。タイプの項目は、テーブルのエントリーのタイプを表わすものであり、「アクティブ（Active）」あるいは「通常（Regular ）」のいずれかの値をとる。宛先アドレスおよび送信元アドレスの項目は、転送対象のパケットの宛先ＩＰアドレスおよび送信元ＩＰアドレスにそれぞれ対応するものである。転送先の項目はは、宛先アドレスと送信元アドレスの組み合せがマッチしたパケットに関して、適用すべきアクティブコードの識別情報あるいは転送先の通信装置のＩＰアドレスを表わすものである。

【００７３】タイプの値が「アクティブ」であるエントリーは、対象のパケットに適用するアクティブコードを指定するものであり、その転送先の項目にはアクティブコードを識別する情報が書かれている。タイプの値が「通常」であるエントリーは、対象のパケットの転送先の通信装置のアドレスを指定するものであり、その転送先の項目には転送先の通信装置のＩＰアドレスが書かれている。

【００７４】図１１に示す転送先テーブルの例において、第１のエントリーでは、タイプが「アクティブ」であり、宛先アドレスが「１．２．３．４」であり、送信元アドレスが「Ａｎｙ（何でもよい）」であり、転送先が「アクティブコードＡ」となっている。これは、送信元アドレスがいかなるアドレスであっても、宛先アドレスが「１．２．３．４」にマッチする場合には、該当するパケットをトリガーとしてアクティブネットワーク実行環境が起動され、アクティブコードＡが実行されることを表わしている。また、第２のエントリーでは、タイプが「アクティブ」であり、宛先アドレスが「１０．５０．０．０」であり、送信元アドレスが「１１．１２．１３．１４」であり、転送先が「アクティブコードＢ」となっている。これは、宛先アドレスと送信元アドレスの両方がそれぞれ上記の値にマッチした場合には、該当するパケットをトリガーとしてアクティブネットワーク実行環境が起動され、アクティブコードＢが実行されることを表わしている。また、第３のエントリーでは、タイプが「アクティブ」であり、宛先アドレスが「Ａｎｙ（何でもよい）」であり、送信元アドレスが「１５７．２．３．０」であり、転送先が「アクティブコードＣ」となっている。これは、宛先アドレスがいかなるアドレスであっても、送信元アドレスが「１５７．２．３．０」にマッチする場合には該当するパケットをトリガーとしてアクティブネットワーク実行環境が起動され、アクティブコードＣが実行されることを表している。

【００７５】なお、図１１に示すように、転送先テーブルにおいては、タイプが「アクティブ」であるエントリーのほうが、タイプが「通常」であるエントリーよりも上に存在している。そして、タイプが「アクティブ」であるエントリーのほうが、タイプが「通常」であるエントリーよりも優先的に適用される。また、各エントリーは、通信装置へ到着したパケットのみに対して適用され、転送のために送出されるパケットに対しては適用されない。

【００７６】以上説明した通信装置の構成をまとめる。図１０に示したインタフェース部は、通信線毎に設けられており、当該通信線から到着するパケットを受信するとともに当該通信線に対してパケットを送出する処理を行う。また、転送先テーブル記憶部は、パケットの送信元アドレスまたは宛先アドレスまたはそれら両方のアドレスのパターンと、該パターンに対応するプログラム（アクティブコード）の情報あるいは該パターンに対応する転送先アドレスの情報とが登録された転送先テーブルを記憶する。また、アクティブネットワーク実行環境は、前記プログラムを予め記憶しているとともに、このプログラムを実行する。また、転送処理部は、通信線から到着した受信パケットを前記インタフェース部から渡された際に、当該受信パケットの送信元アドレスまたは宛先アドレスに基づいて前記転送先テーブルを参照し、前記転送先テーブルに当該受信パケットのアドレスのパターンに対応する転送先アドレスの情報が登録されていた場合には当該受信パケットを所定の転送先アドレスに向けて送出するように当該転送先アドレスに対応したインタフェース部に渡すとともに、前記転送先テーブルに当該受信パケットのアドレスのパターンに対応するプログラムの情報が登録されていた場合には前記アクティブネットワーク実行環境部において当該プログラムを起動させるとともに当該プログラムに当該受信パケットを渡す。

【００７７】次に、本実施形態におけるアクティブコードのセキュリティに関するモデルについて説明する。このセキュリティのモデルは、各々のアクティブコードが、アクティブコードの所有者に関わるパケットのみに対して作用することを保証するためのものである。そのために、このセキュリティのモデルは、公開鍵のインフラストラクチャの存在を前提として、それを利用することとする。

【００７８】図１２は、上記のセキュリティモデルとそのモデルにおける処理の手順を示す概略図である。図１２において、符号７０５１はユーザＡのユーザ端末装置、７０６１は認証局（Certification Authority ）装置である。この認証局の機能は、公の機関によって提供

されるものであっても良いし、あるいはＩＳＰ（Internet Service Provider,インターネット接続サービス提供者）などによって提供されるものであっても良い。なお、図１２に示す例では、ユーザ端末装置７０５１のＩＰアドレスは「１．２．３．４」である。以下では、ユーザＡが、アクティブコードＡを通信装置７００１に登録するための処理の手順を説明する。なお、以下において、ユーザＡはアクティブコードＡの開発者であっても良いが、その必然性はなく、他の開発者が開発したアクティブコードＡをユーザＡが入手し、それを通信装置７００１に登録するものでも良い。

【００７９】まず（１）で示すように、ユーザＡのユーザ端末装置７０５１は、周知技術を用いて鍵のペアすなわち公開鍵と秘密鍵とを生成する。そして（２）で示すように、ユーザ端末装置７０５１は、上で生成された公開鍵を認証局装置７０６１に登録する。このとき、認証局装置７０６１は、ユーザ端末装置７０５１のＩＰアドレスを検証する。この検証が正しく行なわれると、公開鍵そのものと、ユーザＡを識別するための情報と、ユーザ端末装置７０５１のＩＰアドレス「１．２．３．４」が認証局装置７０６１に記憶される。

【００８０】次に（３）で示すように、ユーザ端末装置７０５１は、上で生成された秘密鍵を用いてアクティブコードＡに電子署名する処理を行う。そして（４）で示すように、ユーザ端末装置７０５１は、秘密鍵で署名されたアクティブコードＡを通信装置７００１に登録する処理を行う。

【００８１】これを受けて通信装置７００１は、（５）で示すように、アクティブコードＡの登録を行ったユーザＡの電子証明書を認証局装置７０６１から取得する。この電子証明書には、ユーザＡを識別する情報と、そのＩＰアドレス「１．２．３．４」と、上の（２）において登録された公開鍵そのものとが含まれている。そして（６）で示すように、通信装置７００１は、上記の電子証明書から取り出したユーザＡの公開鍵を用いて、上の（４）において登録されたアクティブコードＡの電子署名を検証する。そして、これが正しく検証された場合には、通信装置７００１は、アクティブコードＡをアクティブネットワーク実行環境に導入する処理を行う。また、これに応じて、転送先テーブルに必要なエントリーが追加される。

【００８２】なお、この（１）および（２）の処理が行われて一旦ユーザＡの公開鍵が認証局装置７０６１に登録されると、ユーザ端末装置７０５１はその公開鍵に対応する秘密鍵を用いてアクティブモジュールをいくつでも通信装置７００１に登録することも可能である。

【００８３】つまり、通信装置７００１は登録部（図示せず）を備えており、この登録部は、ユーザの端末装置から当該ユーザの秘密鍵で電子署名されたプログラムを受信し、当該ユーザの電子証明書を認証局装置から受信し、受信した電子証明書に含まれる当該ユーザの公開鍵を用いて前記電子署名されたプログラムの検証を行い、この検証が成功した場合には当該プログラムに対応するアドレスのパターンと当該プログラムの情報とを前記転送先テーブルに登録し、この検証が失敗した場合には当該プログラムの情報の前記転送先テーブルへの登録は行わないようにするものである。

【００８４】なお、上で説明した通信装置へのアクティブコードの登録の手順が行効に機能するためには、次の２点が前提となる。第１の前提として、ユーザがどの通信装置（ノード）にアクティブコードを登録すれば良いかは事前にわかっている。あるいは、どの通信装置（ノード）にアクティブコードを登録すればよいかがわかるためのディレクトリサービスが提供されている。第２の前提として、通信装置（ノード）は、目的の認証局の公開鍵を事前にオフラインで取得しているか、他の認証局から取得するか、あるいは他の何らかの手段で取得できる。

【００８５】次に、矛盾の解消のための制御について説明する。ある通信装置（ノード）において、ｎ個のアクティブコードが登録されており、ｉ番目（１≦ｉ≦ｎ）とｊ番目（１≦ｊ≦ｎ）のアクティブコードが、それぞれ集合Ｃ（ｉ）（Ｃ（ｉ）⊆Ａ）と集合Ｃ（ｊ）（Ｃ（ｊ）⊆Ａ）に属するパケットに対するものであると定義されているとき、集合（ｃ（ｉ）∩ｃ（ｊ））が空集合ではないようなｉおよびｊの組み合せ（但しｉ≠ｊ）が存在する場合があり得る。つまり、あるパケットがｉ番目のアクティブコードにもｊ番目のアクティブコードにも適用されるような定義が行われている場合である。このような矛盾は、次の２通りのシナリオのいずれかによって解消することとする。

【００８６】第１の矛盾の解消のシナリオは、パケット（ｓ，ｄ）に関して、

（ｓ∈Ｏ（ｋ）∧ｄ∈Ｏ（ｌ））∧（ｋ≠ｌ）

であるために、

（ｓ，ｄ）∈ｃ（ｉ）∩ｃ（ｊ）

となる場合に関するものである。但し、Ｏ（ｋ）およびＯ（ｌ）は、それぞれユーザｋおよびｌによって所有されるＩＰアドレスの集合である。つまり、あるパケットに関して、送信元のユーザ用のアクティブコードと宛先のユーザ用のアクティブコードとの両方が通信装置に登録されており、そのような通信装置にこのパケット（ｓ，ｄ）が到着した場合である。このような場合には、宛先のユーザのアクティブコードを優先的に適用することが望ましいと考えられる。

【００８７】つまり、転送先テーブルに登録されているパターンに、送信元アドレスのみが指定されていて宛先アドレスが何でもよいとされている第１のエントリーと、宛先アドレスのみが指定されていて送信元アドレスが何でもよいとされている第２のエントリーとが含まれ

ており、受信パケットがこれら第１のエントリーと第２のエントリーとの両方にマッチしたときには、第１のエントリーよりも第２のエントリーを優先させて、当該第２のエントリーのパターンに対応するプログラムを起動するようにする。

【００８８】このように、送信元のユーザのアクティブコードよりも宛先のユーザのアクティブコードを優先させることは、アクティブネットワークの機能を用いてＤＤｏＳ（分散型ＤｏＳ，Distributed Denial of Service）攻撃を防御するメカニズムを構築する場合に特に重要となる。そのようにすることによって、宛先のユーザつまり被攻撃者となり得る者のアクティブコードが、攻撃者となる可能性があるもののアクティブコードよりも優先されるためである。

【００８９】第２の矛盾の解消のシナリオは、あるパケット（ｓ，ｄ）に関して適用されるべき２つ以上のアクティブコードが同一のユーザによって登録されている場合に関するものである。このような場合には、該当するアクティブコードのうちの最も古く登録されたものが、他のものよりも優先的に適用されるようにすることが望ましいと考えられる。こうすることにより、ユーザが新しいアクティブコードを登録しようとする際には、新しいアクティブコードを有効にするために事前に古いアクティブコードを削除することが保証されるからである。

【００９０】次に、これまでに述べたようなアクティブネットワークのノードとして機能する通信装置のインプリメンテーションの例について説明する。図１３は、Ｌｉｎｕｘ上のＪａｖａ（登録商標）仮想マシン（ＪＶＭ）を用いてアクティブパケットの処理を行う通信装置を実現した場合の概略図である。

【００９１】図１３に示す例では、専用のＩＰスタックを処理（process）の一部として構築している。これによって、図１１に示したような転送先テーブルを実現し、実行環境（アクティブネットワーク実行環境）からこの転送先テーブルにエントリーの追加や削除を行えるようにしている。また、これに伴い、カーネル（kernel）内のＩＰスタックは不要となるため、カーネルにおけるルーティングを不活性化している。そして、到着パケットのコピーがデータリンク部分から作成され、そのパケットがライブラリｌｉｂｐｃａｐを通してＪａｖａ（登録商標）仮想マシンで補足できるようにしている。

【００９２】処理の一部として構築した専用のＩＰスタックは、アクティブパケット、つまり転送先テーブル上での所定の定義にマッチするＩＰアドレス（宛先ＩＰアドレス、送信元ＩＰアドレス、あるいはそれらの組み合せ）を有するパケットは、実行環境上で起動されるアクティブコードに対して渡される。一方、アクティブパケット以外の通常のパケットは、カーネルにおけるＩＰスタックと同様の方法で隣接する通信装置等へ向けた転送が行われる。アクティブパケットであれ通常パケットであれ、この通信装置から送出されるすべてのパケットは、ライブラリｌｉｂｎｅｔを通して送出される。こうすることにより、各々処理されたパケットのヘッダに記録された送信元アドレスは、元々の送信元アドレスのままの状態で、ネットワークに送出されることとなる。

【００９３】また、標準のＪａｖａ（登録商標）のＡＰＩ（アプリケーションプログラムインタフェース）である「java.security」を用いることによってセキュリティモデルをインプリメンテーションすることが可能である。この標準ＡＰＩは、セキュリティモデルを構築するために必要な機能のほとんどを提供している。また、証明書のための形式としては「Ｘ．５０９」証明書形式を用いることが可能であり、アクティブコードの所有者のＩＰアドレスを「Ｘ．５０９」の識別名（ＤＮ，distinguished name）の一部に含めることにより、本実施形態のセキュリティモデルを実現することができる。

【００９４】なお、言うまでもなく、上記インプリメンテーションではコンピュータシステムを用いることによってアクティブネットワーク実行環境を備えた通信装置を構築している。そして、上述した一連の処理、すなわち到着パケットの複製の作成とその捕捉や、転送先テーブルを参照しながらのアクティブパケットおよび通常パケットの転送の処理や、アクティブネットワーク実行環境上でのアクティブコードの起動とその処理の実行や、処理されたパケットのネットワークへの送出などの各処理の過程は、プログラムの形式でコンピュータ読み取り可能な記録媒体に記憶されており、このプログラムをコンピュータが読み出して実行することによって、上記処理が行われる。ここでコンピュータ読み取り可能な記録媒体とは、磁気ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、ＤＶＤ－ＲＯＭ、半導体メモリ等をいう。また、このコンピュータプログラムを通信回線によってコンピュータに配信し、この配信を受けたコンピュータが当該プログラムを実行するようにしても良い。

【００９５】以上、図面を参照してこの発明の実施形態を詳述してきたが、具体的な構成はこれらの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。例えば、上記実施形態ではインターネットプロトコルの使用を前提として通信アドレスを４バイトのＩＰアドレスとして書き表したが、より多いバイト数のアドレスを用いる次世代のＩＰや、まったく異なる他のプロトコルを用いる通信ネットワークにも本発明を適用することができる。

【００９６】

【発明の効果】以上説明したように、この発明によれば、シールド通信装置が、到着する通信パケットを分析する分析処理を行い、この分析処理の結果に応じて当該通信パケットが前記防御対象コンピュータに対する攻撃の通信パケットである可能性に応じて当該通信パケットの優先度を決定してこの優先度に応じて当該通信パケッ

トを転送先に転送するようにしている。このため、従来技術において攻撃のパケットであるか否かを二値的に判断して処理していたのに比べると、攻撃下において正常な通信パケットが届きにくくなるというダメージを最小化することができる。また、攻撃のパケットであるかどうかを確定できない段階においても、疑わしい通信パケットが占めるの帯域を段階的に絞っていくことができる。

【００９７】また、この発明によれば、境界通信装置から最も遠い位置にあるシールド通信装置との間の接続の段数として２以上を許容しているため、つまりシールド通信装置の段数（深さ）を２以上にできるため、防御の処理の負荷を分散させることができるとともに、より攻撃元に近い位置で防御を行うため、下流側の通信線の帯域を浪費せずに有効に使うことができる。

【００９８】また、この発明によれば、攻撃が検出されたときに、シールド通信装置からより上流へプローブの機能を段階的に移動させていくため、より攻撃元に近い場所での防御が可能となる。これにより、下流側の通信線の帯域を有効に使うことができるとともに、攻撃元に関する経路情報を収集する処理を行うことができる。

【００９９】また、この発明によれば、プローブの処理として、宛先アドレスが防御対象コンピュータのアドレスである通信パケットを捕捉し、当該通信パケットの送信元アドレスが予め得られた攻撃元のアドレスと同一である場合には当該通信パケットが攻撃のパケットであると判定するようにしているため、実施形態の説明に記載したＡ型のＤＤｏＳ攻撃を防御することができる。

【０１００】また、この発明によれば、プローブの処理として、宛先アドレスあるいは送信元アドレスの少なくともいずれか一方が前記防御対象コンピュータのアドレスである通信パケットを捕捉し、当該通信パケットの送信元アドレスが防衛対象コンピュータのアドレスであって且つ当該通信パケットの宛先アドレスが前記攻撃元アドレスのブロードキャストアドレスである場合にもこの通信パケットが攻撃のパケットであると判定するため、実施形態の説明に記載したＢ型のＤＤｏＳ攻撃を防御することができる。

【０１０１】また、この発明によれば、動的検査を導入したことにより、従来技術では検知できなかった攻撃も検知して防御できるようになった。

【図面の簡単な説明】

【図１】　この発明の一実施形態が前提とするネットワークの構成である。

【図２】　同実施形態による通信装置の内部の構成を示すブロック図である。

【図３】　同実施形態による防御のしくみを示す論理的概略図である。

【図４】　同実施形態のシールドモジュールによる通信パケットのクラス分けの処理の概要を示す概略図である。

【図５】　同実施形態によるシールドモジュールが動的検査を行う場合に用いる送信元ＩＰアドレスの分布状況を示すグラフであり、（ａ）は正常時の分布、（ｂ）は攻撃を受けているときの分布の一例を示す。

【図６】　Ａ型のＤＤｏＳ攻撃を示す概略図である。

【図７】　Ｂ型のＤＤｏＳ攻撃を示す概略図である。

【図８】　本発明の一実施形態により、Ａ型のＤＤｏＳ攻撃に対応するためのプローブのアルゴリズムを記述した擬似プログラムコードである。

【図９】　同実施形態により、Ｂ型のＤＤｏＳ攻撃に対応するためのプローブのアルゴリズムを記述した擬似プログラムコードである。

【図１０】　同実施形態による通信装置内部の構成を示すブロック図である。

【図１１】　同実施形態による転送先テーブル記憶部に記憶されている転送先テーブルの一例を示す概略図である。

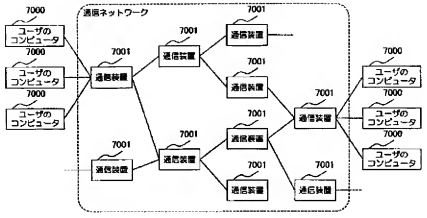
【図１２】　同実施形態によるセキュリティモデルとそのモデルにおける処理の手順を示す概略図である。

【図１３】　同実施形態の通信装置をＬｉｎｕｘ上のＪａｖａ（登録商標）仮想マシン（ＪＶＭ）を用いてアクティブパケットの処理を行うように実現した場合の概略図である。

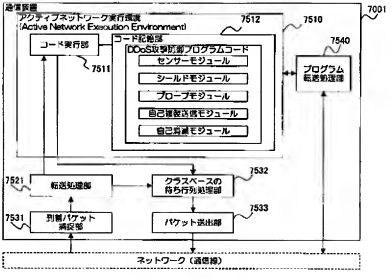
【符号の説明】

７０００　ユーザのコンピュータ
７００１　通信装置
７０１０　アクティブネットワーク実行環境
７０１１　コード実行部
７０１２　コード記憶部
７０２１　転送処理部
７０２２　転送先テーブル記憶部
７０２３ａ、７０２３ｂ、・・・・・・　インタフェース部
７０２４ａ、７０２４ｂ、・・・・・・　通信線
７０５１　ユーザ端末装置
７０６１　認証局装置
７５１０　アクティブネットワーク実行環境
７５１１　コード実行部
７５１２　コード記憶部
７５２１　転送処理部
７５３１　到着パケット捕捉部
７５３２　クラスベースの待ち行列処理部
７５３３　パケット送出部
７５４０　プログラム転送処理部

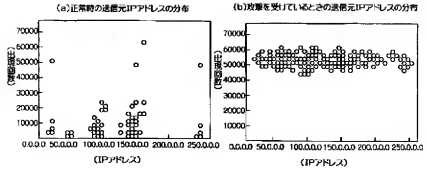
【図１】


通信ネットワーク
7000
ユーザの
コンピュータ
7001
通信装置

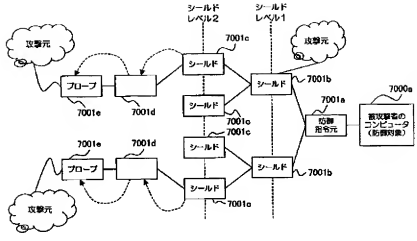
【図２】


通信装置
7001
アクティブネットワーク実行環境
(Active Network Execution Environment)
7512
7510
7540
コード実行部
7511
コード記憶部
DDoS防御部プログラムコード
センサーモジュール
シールドモジュール
プローブモジュール
自己複製送信モジュール
自己修復モジュール
プログラム
転送制御部
7521
転送処理部
7532
クラスベースの
待ち行列処理部
7531
到着パケット
識別部
7533
パケット送出部
ネットワーク（通信線）

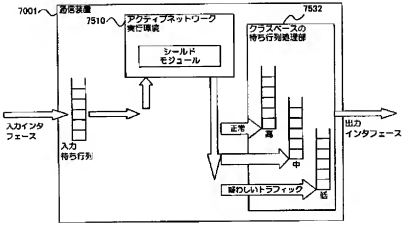
【図５】


(a)正常時の送信元IPアドレスの分布
(b)攻撃を受けているときの送信元IPアドレスの分布
70000
60000
50000
40000
30000
20000
10000
0.0.0.0
50.0.0.0
100.0.0.0
150.0.0.0
200.0.0.0
250.0.0.0
(IPアドレス)

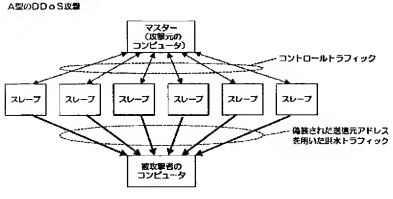
【図３】


シールド
レベル2
シールド
レベル1
攻撃元
攻撃元
7001c
シールド
プローブ
シールド
7001b
7000a
7001a
シールド
攻撃
指令元
被攻撃者の
コンピュータ
（防御対象）
7001c
7001c
7001e
7001d
シールド
7001e
7001d
プローブ
シールド
7001b
シールド
攻撃元
7001a

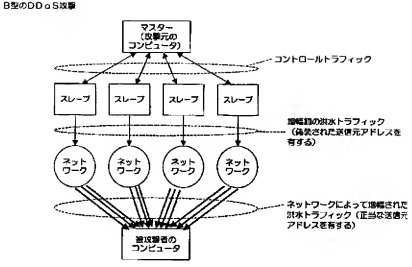
【図４】


7001
通信装置
7510
アクティブネットワーク
実行環境
シールド
モジュール
7532
クラスベースの
待ち行列処理部
入力インタ
フェース
入力
待ち行列
正常
高
中
疑わしいトラフィック
低
出力
インタフェース

【図６】


A型のDDoS攻撃
マスター
（攻撃元の
コンピュータ）
コントロールトラフィック
スレーブ
スレーブ
スレーブ
スレーブ
スレーブ
スレーブ
偽装された送信元アドレス
を用いた攻撃トラフィック
被攻撃者の
コンピュータ

【図７】



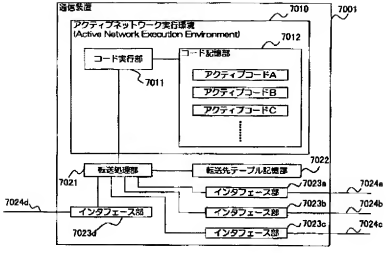
【図８】

```
//Arriving at a new node u
1. explored ← false
2. do
3.     p ← capturePacketByDast(victim's IP)
4.     if p.src=attSrc then
5.         discard(p)
6.         if !explored
7.             for each v∈Adjacent[u]
8.                 if !(v∈predecessor[u]) then
9.                     dispatch a replicate of probe to v
10.    else releasePacket(p)
11.while (p≠NIL) and (!IdleTimeOut)
12.self-destruct
```

【図９】

```
//Arriving at a new node u
1. explored ← false
2. do
3.     p ← capturePacketAssociatedWith(victim's IP)
4.     if (p.src=attSrc) or
       ((p.src=victim's IP)and(p.dest=attSrc's broadcast))
       then
5.         discard(p)
6.         if !explored
7.             for each v∈Adjacent[u]
8.                 if !(v∈predecessor[u]) then
9.                     dispatch a replicate of probe to v
10.    else releasePacket(p)
11.while (p≠NIL) and (!IdleTimeOut)
12.self-destruct
```

【図１０】

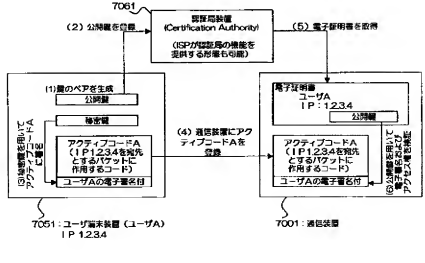


【図１１】

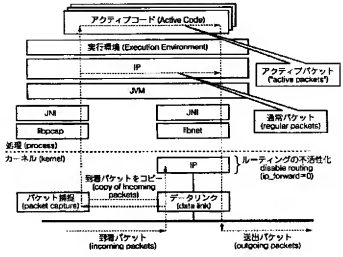
転送先テーブル

タイプ (Type)	宛先アドレス (Destination)	送信元アドレス (Source)	転送先 (Send to)
アクティブ (Active)	1.2.3.4	Any	アクティブコードA
アクティブ	10.50.0.0	11.12.13.14	アクティブコードB
アクティブ	Any	157.23.0	アクティブコードC
通常 (Regular)	1.2.0.0	N/A	29.15.20.1
通常	11.20.0.0	N/A	109.1.1.10
通常	199.1.1.0	N/A	120.0.0.1
.....	.....	.....	.....

【図１２】



【図１３】


アクティブコード (Active Code)
実行環境 (Execution Environment)
IP
JVM
アクティブパケット
(active packets)
JNI
JNI
通常パケット
(regular packets)
libpcap
libnet
処理 (process)
カーネル (kernel)
IP
ルーティングの不活性化
disable routing
(ip_forward=0)
受信パケットをコピー
(copy of incoming packets)
パケット捕捉
(packet capture)
データリンク
(data link)
受信パケット
(incoming packets)
送出パケット
(outgoing packets)